AMENDMENTS TO THE CLAIMS

1   1. (Currently Amended) A method for steganographically combining data, comprising

2   the steps of:

3   acquiring first data via a ~~data source~~ <u>first sensor</u>;

4   *over a* <u>contemporaneously</u> acquiring <u>meta-data associated with the acquired first data via</u>

5   *period of time or a little*   <u>a second sensor</u> ~~from the data source meta-data associated with the~~

6   *or a little later*   ~~acquired first data~~;

7   <u>figure-of-merit testing the acquired first data and the acquired meta-data to</u>

8   <u>determine within what portion of the first data to combine the first data</u>

9   <u>and the acquired data;</u> and

a¹ 10   combining the acquired first data and the acquired meta-data into steganographic

11   data <u>based upon said figure-of-merit testing</u>, wherein a difference between

12   the steganographic data and the acquired first data is imperceptible.

1   2. (Original) The method according to claim 1, further comprising the step of:

2   storing the steganographic data.

1   3. (Original) The method according to claim 2, wherein the steganographic data is

2   stored in memory coupled with the data source.

1   4. (Original) The method according to claim 2, wherein the steganographic data is

2   stored at a location remote from the site where the first data and meta-data are acquired.

1   5. (Original) The method according to claim 1, further comprising the step of:

2   transmitting the steganographic data to the remote location.

2

1   6. (Original) The method according to claim 1, wherein the step of combining produces

2   one or more steganographic data combinations.

1   7. (Original) The method according to claim 6, further comprising the step of:

2   evaluating each of the one or more steganographic data combinations to

3   determine the one combination that most closely matches the acquired first

4   data.

1   8. (Original) The method according to claim 7, further comprising the conditional step

2   of:

3   if all of the one or more steganographic data combinations perceptibly differ from

4   the acquired data, then repeating the step of combining.

1   9. (Original) The method according to claim 1, whereby the step of acquiring meta-data

2   is substantially completed before acquiring another first data.

1   10. (Original) The method according to claim 1, wherein at least a portion of the

2   acquired meta-data is related to information received from a user.

1   11. (Original) The method according to claim 1, wherein:

2   the first data comprises an electro-optical image produced by a component of a

3   digital camera.

1   12. (Currently Amended) The method according to claim 11, wherein:

2   the meta-data relates to one or more of identification of the acquired image,

3   parameter settings of the digital camera, ~~the~~ an environment in which the

4   image is acquired, and a spatial description of the camera.

3

1   13. (Original) The method according to claim 1, further comprising the step of:

2   pre-processing the meta-data by hashing the meta-data, encrypting the meta-data,

3   or encrypting the hashed meta-data.

1   14. (Original) The method according to claim 1, wherein the first data and the meta-data

2   are acquired via the data source at approximately the same time.

1   15. (Currently Amended) A device for generating steganographic data, comprising:

2   a first ~~suite of sensors~~ <u>sensor</u> configured to acquire data;

3   a second ~~suite of sensors~~ <u>sensor</u> configured to <u>contemporaneously</u> acquire meta-

4   data, wherein the meta-data is associated with the acquired data;

5   a steganographic engine configured to combine the acquired data and the acquired

6   meta-data <u>according to the results of a figure-of-merit testing</u> to form

7   steganographic data, wherein the steganographic data differs

8   imperceptibly from the acquired data.

1   16. (Original) The device according to claim 15, further comprising:

2   a memory configured to store the steganographic data.

1   17. (Original) The device according to claim 15, wherein the steganographic data

2   comprises one or more different steganographic data combinations obtained using

3   different combination algorithms.

1   18. (Original) The device according to claim 17, further comprising:

2   a figure-of-merit tester configured to determine one of the one or more

3   steganographic data combinations that differs the least from the acquired

4   data.

1   19. (Currently Amended) The device according to claim 15, wherein the second ~~suite of~~

2   ~~sensors~~ <u>sensor</u> further comprise<u>s</u>:

3   a user interface configured to receive information from a user of the device.

1   20. (Original) The device according to claim 19, wherein the user interface further

2   comprises:

3   one or more different kinds of input devices configured to interact with the user

4   interface.

1   21. (Original) The device according to claim 15, further comprising:

2   a communications interface configured to transmit the steganographic data to a

3   location remote from the device.

1   22. (Currently Amended) The device according to claim 15, wherein the second ~~suite of~~

2   ~~sensors~~ <u>sensor</u> is controlled to complete acquiring the meta-data before the first ~~suite of~~

3   ~~sensors~~ <u>sensor</u> acquires other data.

1   23. (Original) The device according to claim 15, wherein the meta-data comprises

2   hashed and encrypted meta-data portions.

1   24. (Currently Amended) A digital camera for steganographically combining meta-data,

2   comprising:

3   ~~a~~ <u>an</u> image plane configured to acquire an electro-optical image;

4   a ~~suite of sensors~~ <u>sensor</u> configured to <u>contemporaneously</u> acquire meta-data, said

5   meta-data is associated with the electro-optical image;

6   a steganographic engine configured to combine the electro-optical image and the

7   meta-data <u>according to the results of a figure-of-merit test</u> to form

8   steganographic data, said steganographic data differing imperceptibly

9   from the electro-optical image.

1   25. (Original) The digital camera according to claim 24, further comprising:

2   memory configured to store the steganographic data.

1   26. (Original) The digital camera according to claim 24, wherein the steganographic

2   data comprises one or more different steganographic data combinations obtained using

3   different combination algorithms.

1   27. (Original) The digital camera according to claim 26, further comprising:

2   a figure-of-merit tester configured to determine one of the one or more

3   steganographic data combinations that differs the least from the electro-

4   optical image.

1   28. (Original) The digital camera according to claim 24, further comprising:

2   a display area configured to display information related to the meta-data.

1   29. (Original) The digital camera according to claim 24, further comprising:

2   a display area configured to display information related to the steganographic

3   data.

1   30. (Currently Amended) The digital camera according to claim 24, wherein the ~~suite of~~

2   ~~sensors~~ <u>sensor</u> is configured to acquire meta-data related to one or more of camera angle,

3   geographical location, environmental conditions, date and time, image subject

4   identification and image parameter settings.

a'l conc'l

1   31. (Original) The digital camera according to claim 24, wherein the meta-data

2   comprises hashed and encrypted meta-data portions.